

Stefano Suin

Antonio Cisternino

SICUREZZA E DINTORNI, ALL'UNIVERSITÀ DI PISA



ZTA Architecture

- ZT cybersecurity model
 - Traditionally, enterprise networks have focused on perimeter defense and authenticated subjects are given authorized access to a broad collection of resources once on the internal network. As a result, unauthorized lateral movement within the environment has been one of the biggest challenges in cybersecurity
- Cybersecurity architecture based on zero trust principles, so no perimetral security
- Limit internal »lateral« movement (E-W traffic)
- Guidelines principles for workflow system design and operations

Principles and goals

- Trust is never granted implicitly, but must be continually evaluated
- All data sources and computing (physical/virtual) are considered resources
- Prevent unauthorized access to data and services with making dynamic access control enforcement as granular as possible
- All resources authentication and authorization are dynamic and strictly enforced before access is allowed
- All communications are secured regardless of network locations

Logical component of ZTA

- PDP/PEP – Policy Decision/Enforcement point
 - Closer to the resources as much as possible
- Enterprise resources asset
- ID management system
- Data access policies
- Network system and activity log end report

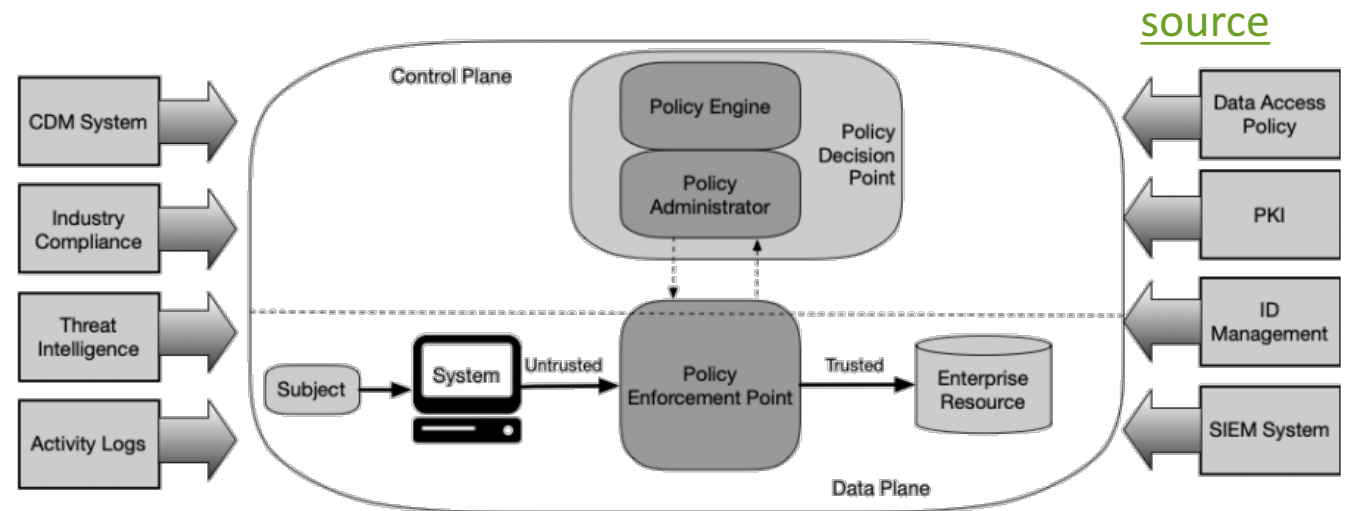


Figure 2: Core Zero Trust Logical Components

ZTA using Micro Segmentation

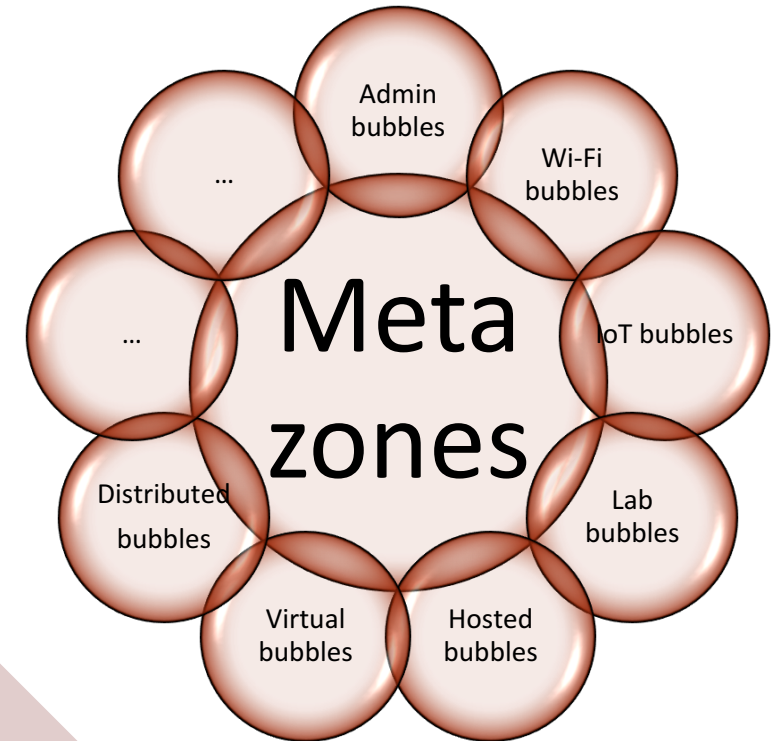
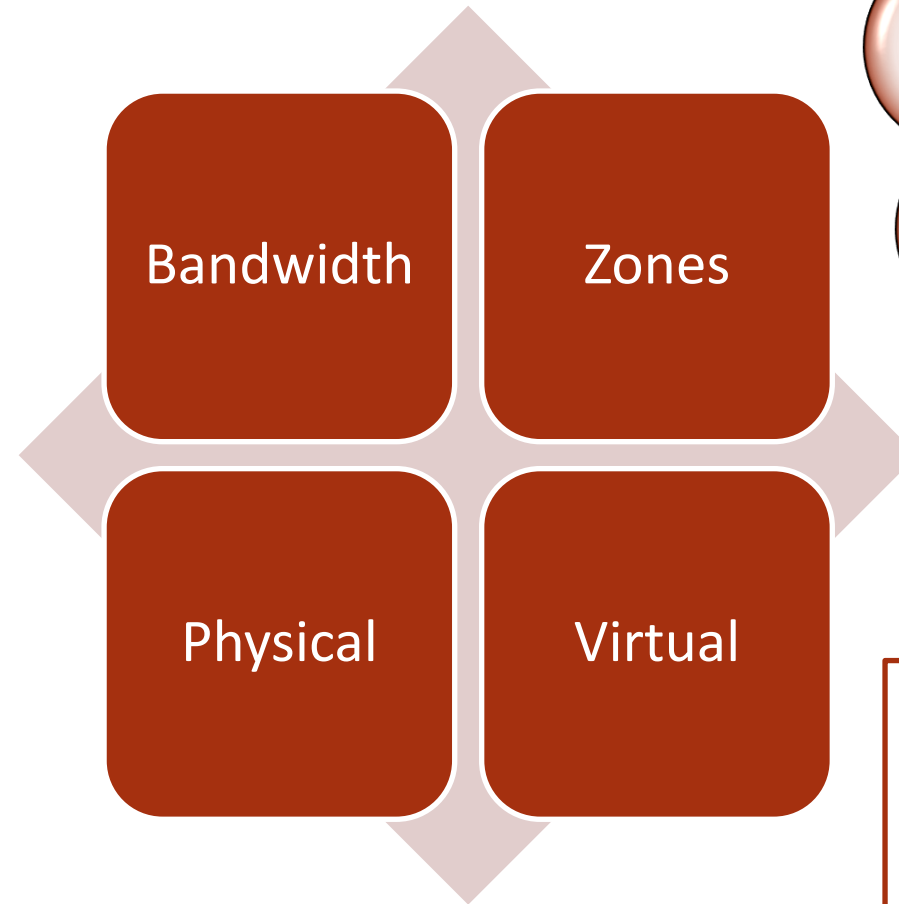
- An institution may choose to implement a ZTA based on placing individual or groups of resources on a unique network segment protected by a gateway security component. In this approach, the enterprise places infrastructure devices such as intelligent switches (or routers) or next generation firewalls (NGFWs) and/or special purpose gateway devices to act as PEPs protecting each resource or small group of related resources.

A Unipi model: BuBbLe security

boundless cybersecurity

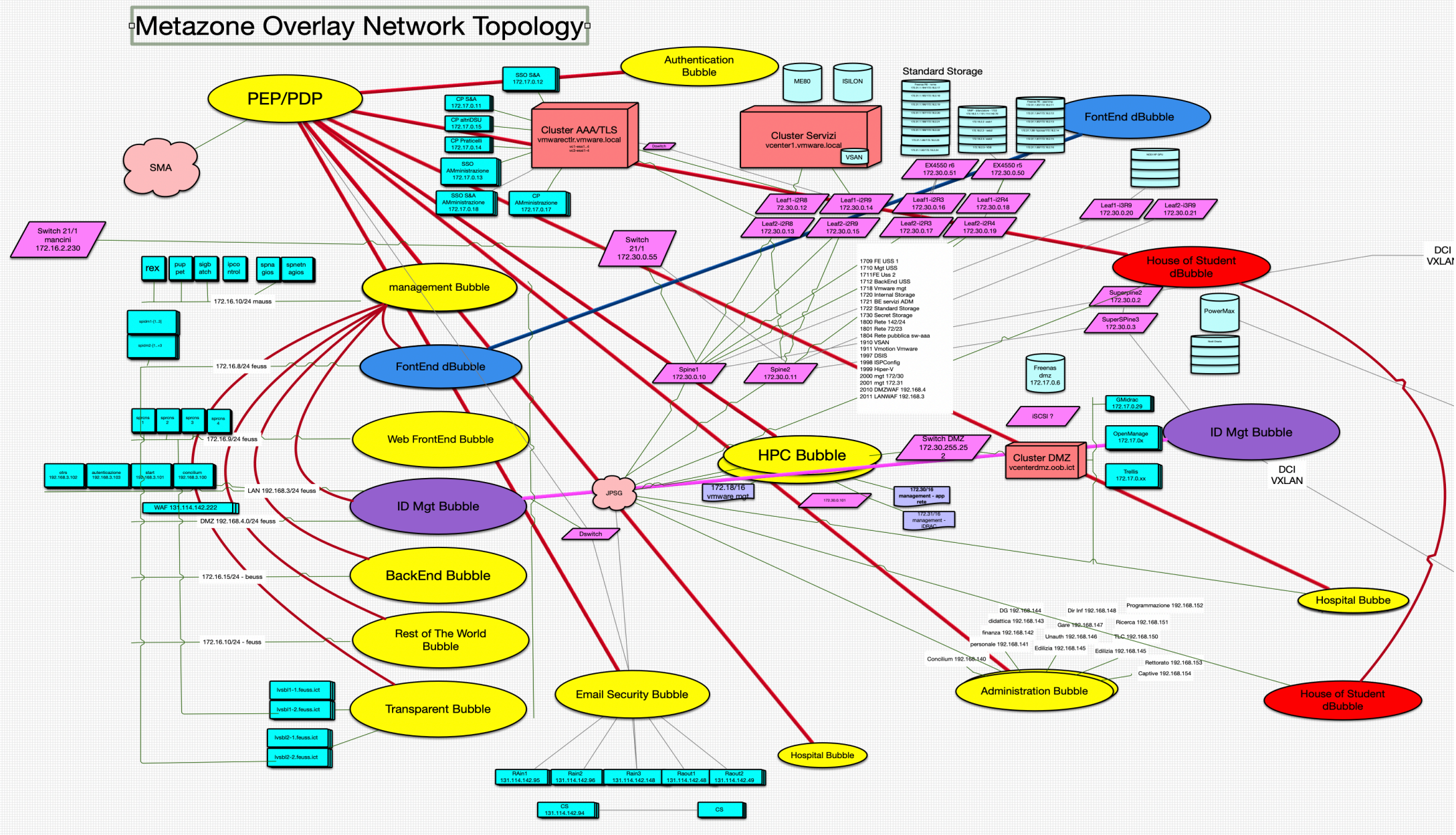
- A set of homogeneous resources protected by a security gateway.
- Each BuBbLe has a defined degree of exposure of its own resources, so called {opacity} of the BuBbLe.
 - Transparent (wired mode)-> Dark (closed Zone)
- Resources in a BuBbLe can be geographically distributed {dBuBbLe}
- Each BuBbLe communicates with others by ipsec tunnels
- All tunnels design an overlay topology so called {MetaZone}
- There is a unique access to the entire MetaZone (PeP/PdP)

BubbleSec



Overlaying security is key to modulate latency and bandwidth and address the eternal tension between security and usability

BuBBle Security



PDP: Resources-Architecture-Identity matrix for enforcement policy

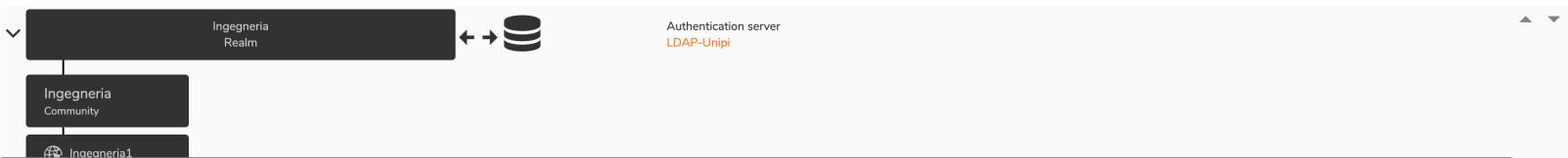
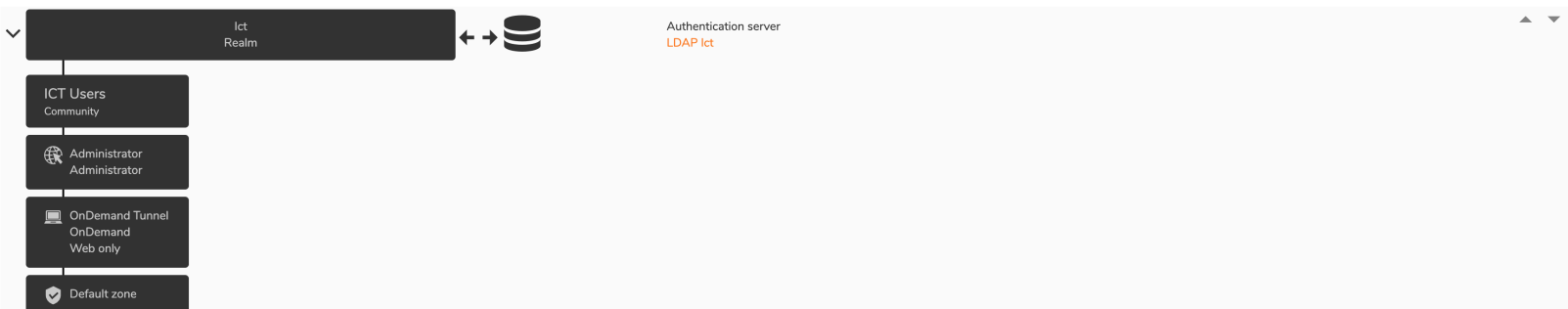
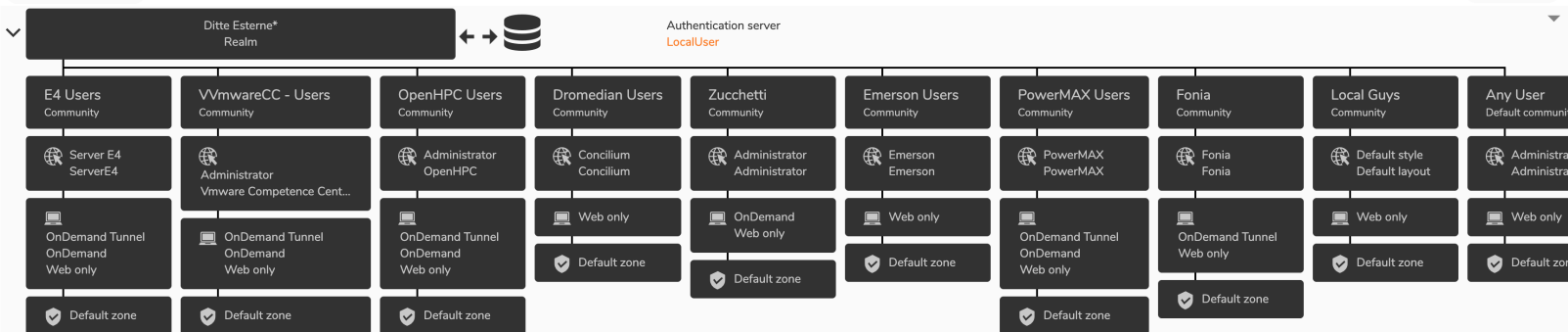
Realms

[Home](#) / [Configure Appliances](#) / [Define Policy](#) / [Realms](#)

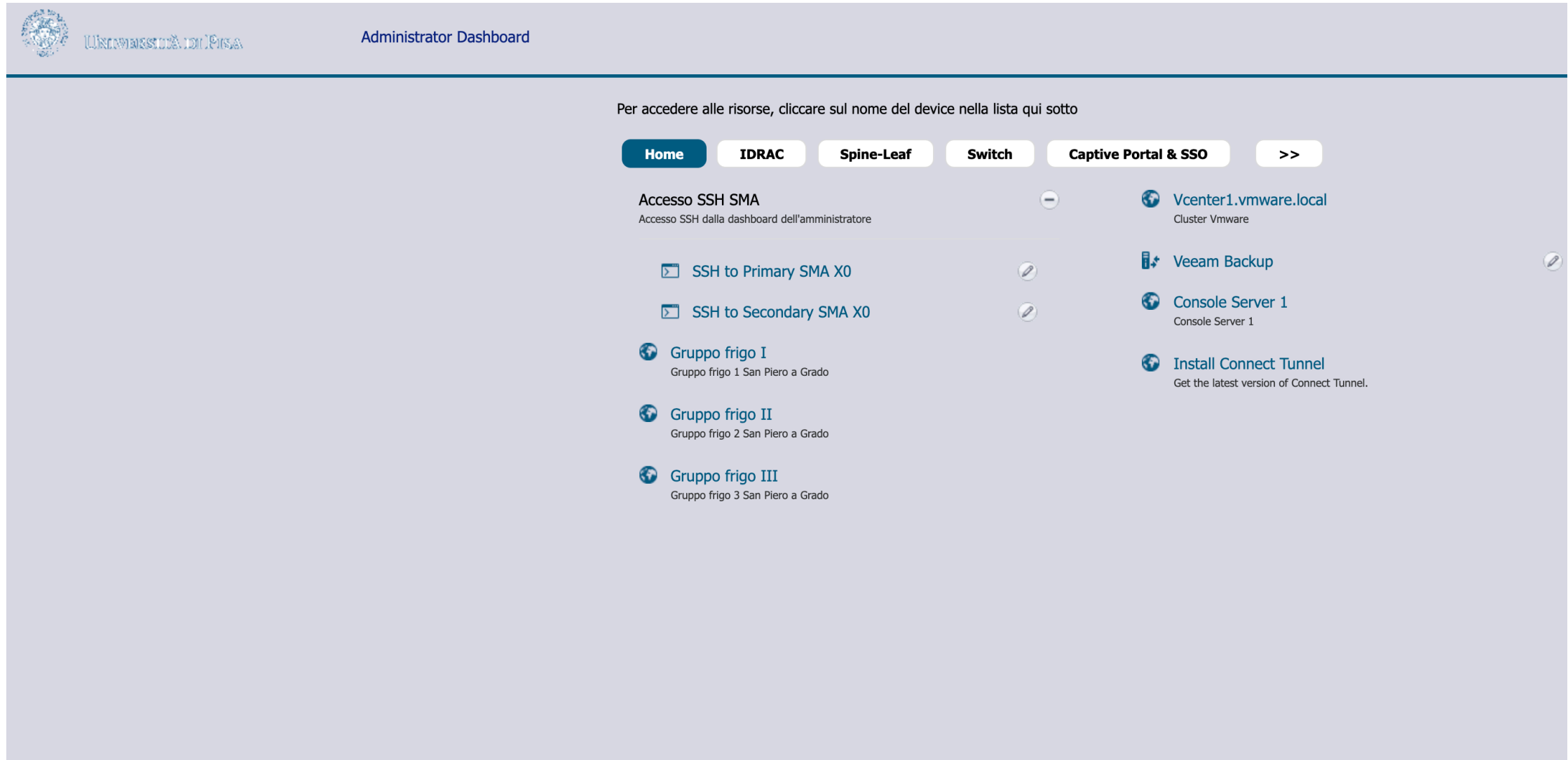
A realm references an authentication server and determines which access agents are provisioned to your users and what end point control restrictions are imposed.

▼ Collapse all details

+ New realm



..and finally...SSO Access to the reosurces (ssh, remote desktop, web access...)






The screenshot displays the 'Administrator Dashboard' of the University of Pisa. At the top left is the university's logo and name. The main navigation bar includes tabs for 'Home', 'IDRAC', 'Spine-Leaf', 'Switch', 'Captive Portal & SSO', and a '>>' button. Below the navigation bar, a message states: 'Per accedere alle risorse, cliccare sul nome del device nella lista qui sotto'. The dashboard is divided into two columns of resource links. The left column contains: 'Accesso SSH SMA' (with a minus icon and description 'Accesso SSH dalla dashboard dell'amministratore'), 'SSH to Primary SMA X0' (with a folder icon and edit icon), 'SSH to Secondary SMA X0' (with a folder icon and edit icon), 'Gruppo frigo I' (with a globe icon and description 'Gruppo frigo 1 San Piero a Grado'), 'Gruppo frigo II' (with a globe icon and description 'Gruppo frigo 2 San Piero a Grado'), and 'Gruppo frigo III' (with a globe icon and description 'Gruppo frigo 3 San Piero a Grado'). The right column contains: 'Vcenter1.vmware.local' (with a globe icon and description 'Cluster Vmware'), 'Veeam Backup' (with a server icon and edit icon), 'Console Server 1' (with a globe icon and description 'Console Server 1'), and 'Install Connect Tunnel' (with a globe icon and description 'Get the latest version of Connect Tunnel.').



University of Pisa Administrator Dashboard


Per accedere alle risorse, cliccare sul nome del device nella lista qui sotto


Home IDRAC Spine-Leaf Switch **Captive Portal & SSO** >>


Accesso SSH SMA 
Accesso SSH dalla dashboard dell'amministratore


 **SSH to Primary SMA X0** 



 **SSH to Secondary SMA X0** 


 **Gruppo frigo I**
Gruppo frigo 1 San Piero a Grado


 **Gruppo frigo II**
Gruppo frigo 2 San Piero a Grado

 **Gruppo frigo III**
Gruppo frigo 3 San Piero a Grado

 **Vcenter1.vmware.local**
Cluster Vmware

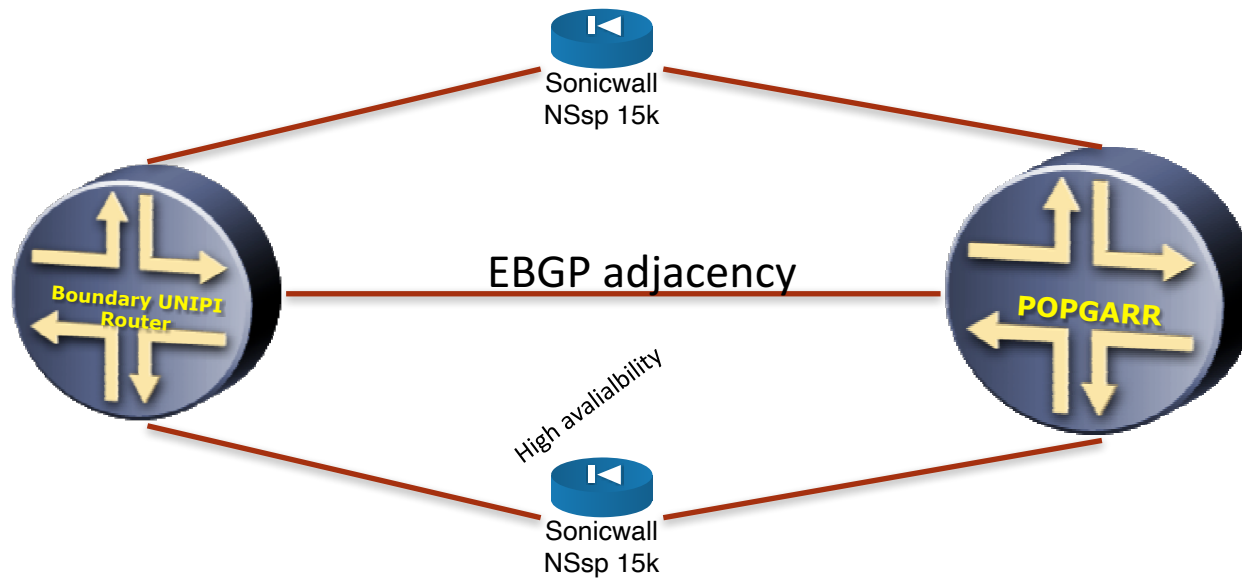
 **Veeam Backup** 

 **Console Server 1**
Console Server 1

 **Install Connect Tunnel**
Get the latest version of Connect Tunnel.

What about boundary?

- Unipi has inserted a Next Generation L7 Firewall in a L2 wired mode – completely transparent -



Advantages

- Simple enforcement policies with large effect
- Perimeter becomes important for monitoring the behavior of the network and the timely identification of anomalies
- Traffic and protocol report of the whole network
- Analytics of the network (user, devices, location, destination, web activities, threats... etc)

Simple enforcement policies with large effect - 1

<div><div><div><div><div></div><div></div></div><div><div></div><div></div></div></div><div><div>Add</div><div>Delete</div></div><div><div>Search...</div></div><div><div>From InternetFrontierExt</div><div>To InternetFrontierInt</div></div><div><div></div><div>IPv4 & IPv6</div></div><div><div>View All Types</div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div>Max Rule Count 22050</div><div></div></div></div></div>																
<input type="checkbox"/>	#	Name	From	To	Priority	Source	Destination	Service	Action	Users Incl.	Users Excl.	Class	Comment	Enabled	Configure	
<input type="checkbox"/>	1	<div>v4</div> Protezione SSH per i firewall sonicwall	InternetFrontierExt	InternetFrontierInt	438 (Manual)	Any	IP SSH SW Group	SSH	Deny	All	None	Custom	<div><div></div><div></div></div>	<input checked="" type="checkbox"/>	<div><div></div><div></div><div></div></div>	
<input type="checkbox"/>	2	<div>v4</div> Protezione SSH interfaccia router.	InternetFrontierExt	InternetFrontierInt	439 (Manual)	Any	Reti Protette SSH	SSH	Deny	All	None	Custom	<div><div></div><div></div></div>	<input checked="" type="checkbox"/>	<div><div></div><div></div><div></div></div>	
<input type="checkbox"/>	3	<div>v4</div> Accesso RDP WEDO	InternetFrontierExt	InternetFrontierInt	440 (Auto)	WEDO Source	WEDO Internal	Terminal Services	<div>Service Properties</div> <div>LDAP: TCP Port 389</div> <div>LDAP (UDP): UDP Port 389</div> <div>LDAPS: TCP Port 636</div> <div>NTP: UDP Port 123</div> <div>Kerberos: <Service Group></div> <div>DCE EndPoint: TCP Port 135</div> <div>Host Name: <Service Group></div> <div>Server: <Service Group></div> <div>AD NetBios Services: <Service Group></div> <div>RPC Services: TCP Ports 1025-5000</div> <div>RPC Services (IANA): TCP Ports 49152-65535</div>	Deny	All	None	Custom	<div><div></div><div></div></div>	<input checked="" type="checkbox"/>	<div><div></div><div></div><div></div></div>
<input type="checkbox"/>	4	<div>v4</div> Chiusura RDP	InternetFrontierExt	InternetFrontierInt	441 (Manual)	Any	Any	Terminal Services		Deny	All	None	Custom	<div><div></div><div></div></div>	<input checked="" type="checkbox"/>	<div><div></div><div></div><div></div></div>
<input type="checkbox"/>	5	<div>v4</div> Chiusura Netbios	InternetFrontierExt	InternetFrontierInt	442 (Manual)	Any	Any	NetBios		Deny	All	None	Custom	<div><div></div><div></div></div>	<input checked="" type="checkbox"/>	<div><div></div><div></div><div></div></div>
<input type="checkbox"/>	6	<div>v4</div> Software Erasmus	InternetFrontierExt	InternetFrontierInt	443 (Manual)	Azure Network	ErasmusDB	RPC Services		Deny	All	None	Custom	<div><div></div><div></div></div>	<input checked="" type="checkbox"/>	<div><div></div><div></div><div></div></div>
<input type="checkbox"/>	7	<div>v4</div> Funzionamento ESSETRE	InternetFrontierExt	InternetFrontierInt	444 (Auto)	Any	ESSETRE	RPC Services		Deny	All	None	Custom	<div><div></div><div></div></div>	<input checked="" type="checkbox"/>	<div><div></div><div></div><div></div></div>
<input type="checkbox"/>	8	<div>v4</div> Protezione Ad directory Services su reti applicative	InternetFrontierExt	InternetFrontierInt	445 (Auto)	Any	Reti Supporto Applicazioni	AD Directory Services	Deny	All	None	Custom	<div><div></div><div></div></div>	<input checked="" type="checkbox"/>	<div><div></div><div></div><div></div></div>	
<input type="checkbox"/>	9	<div>v4</div> Blocco raggiungibilità HOST da Internet	InternetFrontierExt	InternetFrontierInt	446 (Manual)	Any	BlockedFromEXT	Any	Deny	All	None	Custom	<div><div></div><div></div></div>	<input checked="" type="checkbox"/>	<div><div></div><div></div><div></div></div>	
<input type="checkbox"/>	10	<div>v4</div>	InternetFrontierExt	InternetFrontierInt	447 (Manual)	Any	Any	Any	Allow	All	None	Default	<div><div></div><div></div></div>	<input checked="" type="checkbox"/>	<div><div></div><div></div><div></div></div>	
<input type="checkbox"/>	11	<div>v6</div>	InternetFrontierExt	InternetFrontierInt	685 (Manual)	Any	Any	Any	Allow	All	None	Default	<div><div></div><div></div></div>	<input checked="" type="checkbox"/>	<div><div></div><div></div><div></div></div>	

Simple enforcement policies with large effect

Geo IP

Status: ● Active

Note: If you believe that a certain address is marked as part of a country incorrectly, you can go to [Geo-IP Status Lookup](#) to report this issue

Countries
























Custom List

Web Block Page

Diagnostics

Settings

Countries

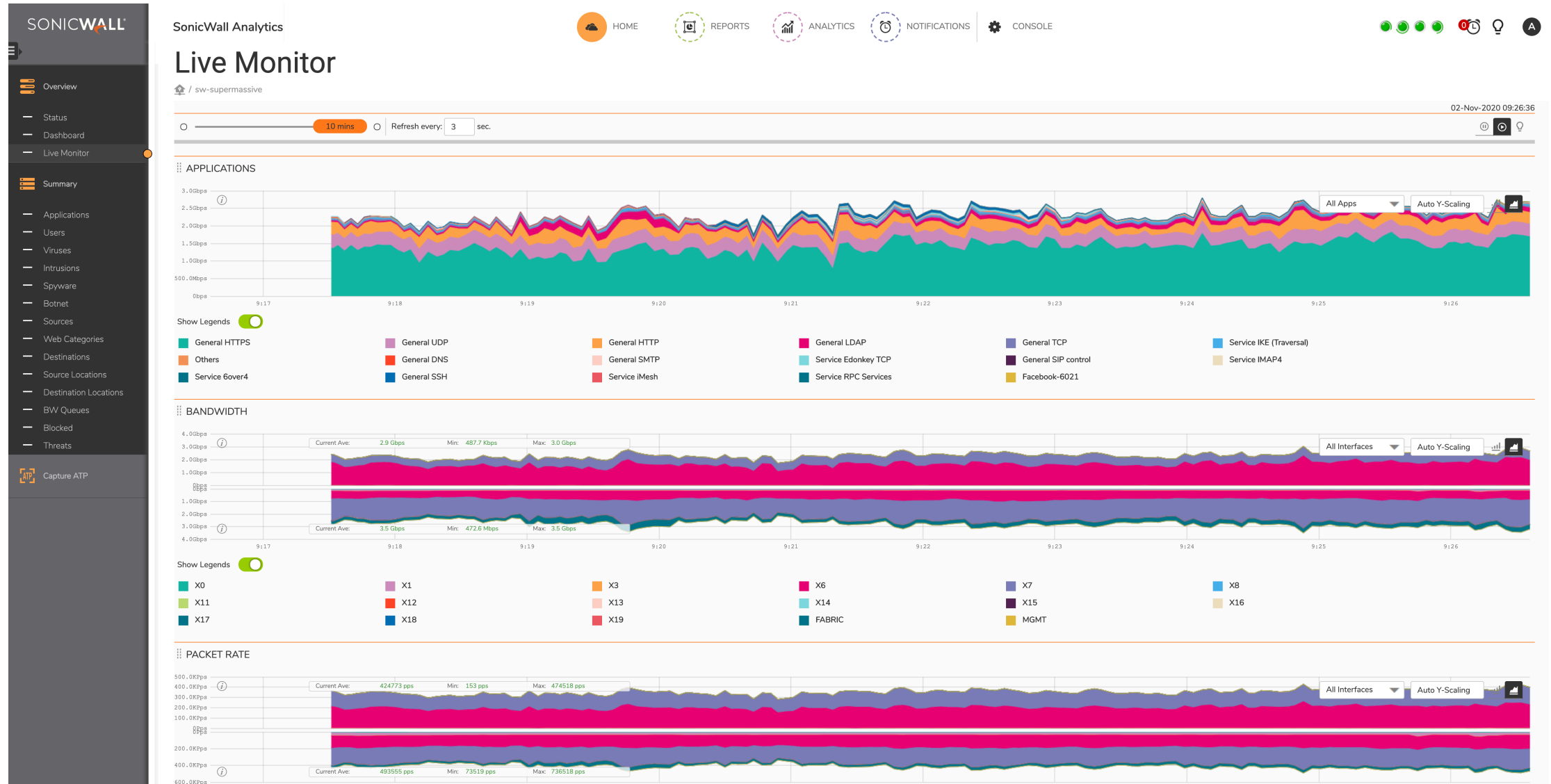
Allowed Countries:	Blocked Countries:
<div><div> Portugal</div><div> Puerto Rico</div><div> Qatar</div><div> Reunion</div><div> Romania</div><div> Rwanda</div><div> Saint Helena</div><div> Saint Kitts and Nevis</div><div> Saint Lucia</div><div> Saint Martin</div><div> Saint Pierre and Miquelon</div><div> Saint Vincent and the Grenadine</div><div> Samoa</div><div> San Marino</div><div> Sao Tome and Principe</div><div> Satellite Provider</div><div> Saudi Arabia</div><div> Senegal</div><div> Serbia</div><div> Seychelles</div></div>	<div><div> China</div><div> Lithuania</div><div> Russian Federation</div></div>

☐ Block All UNKNOWN countries

Geo-IP Exclusion Object

Default Geo-IP and Botnet Exclusion Group

Live Monitor of the network



Live monitoring application detail

SONICWALL

Overview

Status

Dashboard

Live Monitor

Summary

Applications

Users

Viruses

Intrusions

Spyware

Botnet

Web Categories

Sources

Destinations

Source Locations

Destination Locations

BW Queues

Threats

Blocked

Capture ATP

SonicWall Analytics



HOME



REPORTS



ANALYTICS



NOTIFICATIONS



CONSOLE



Applications

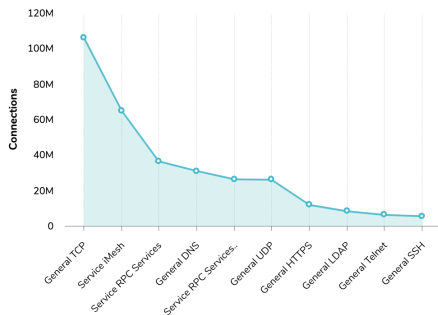
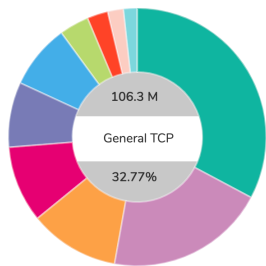
Tenant - LocalDomain / sw-supermassive

6 Hours Custom

TOP APPLICATIONS BY CONNECTIONS

	APPLICATIONS NAME	CONNECTIONS	PERCENTAGE
<input type="checkbox"/>	8.8.8.8	9.3 M	46.35%
<input type="checkbox"/>	131.114.142.20	2.9 M	14.69%
<input type="checkbox"/>	131.114.142.19	2.9 M	14.66%
<input type="checkbox"/>	131.114.209.2...	960.7 K	4.79%
<input type="checkbox"/>	131.114.73.222	803.5 K	4.00%
<input type="checkbox"/>	131.114.21.5	700.5 K	3.49%
<input type="checkbox"/>	131.114.21.10	658.2 K	3.28%
<input type="checkbox"/>	131.114.2.138	610.5 K	3.04%
<input type="checkbox"/>	131.114.3.48	573.1 K	2.86%
<input type="checkbox"/>	131.114.3.17	571.8 K	2.85%

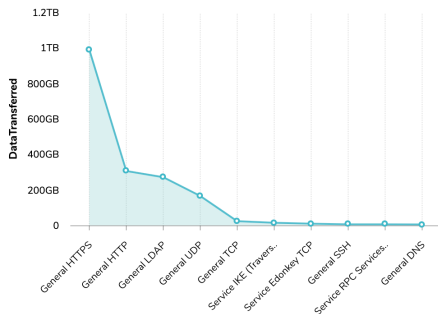
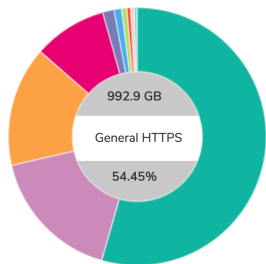
details...



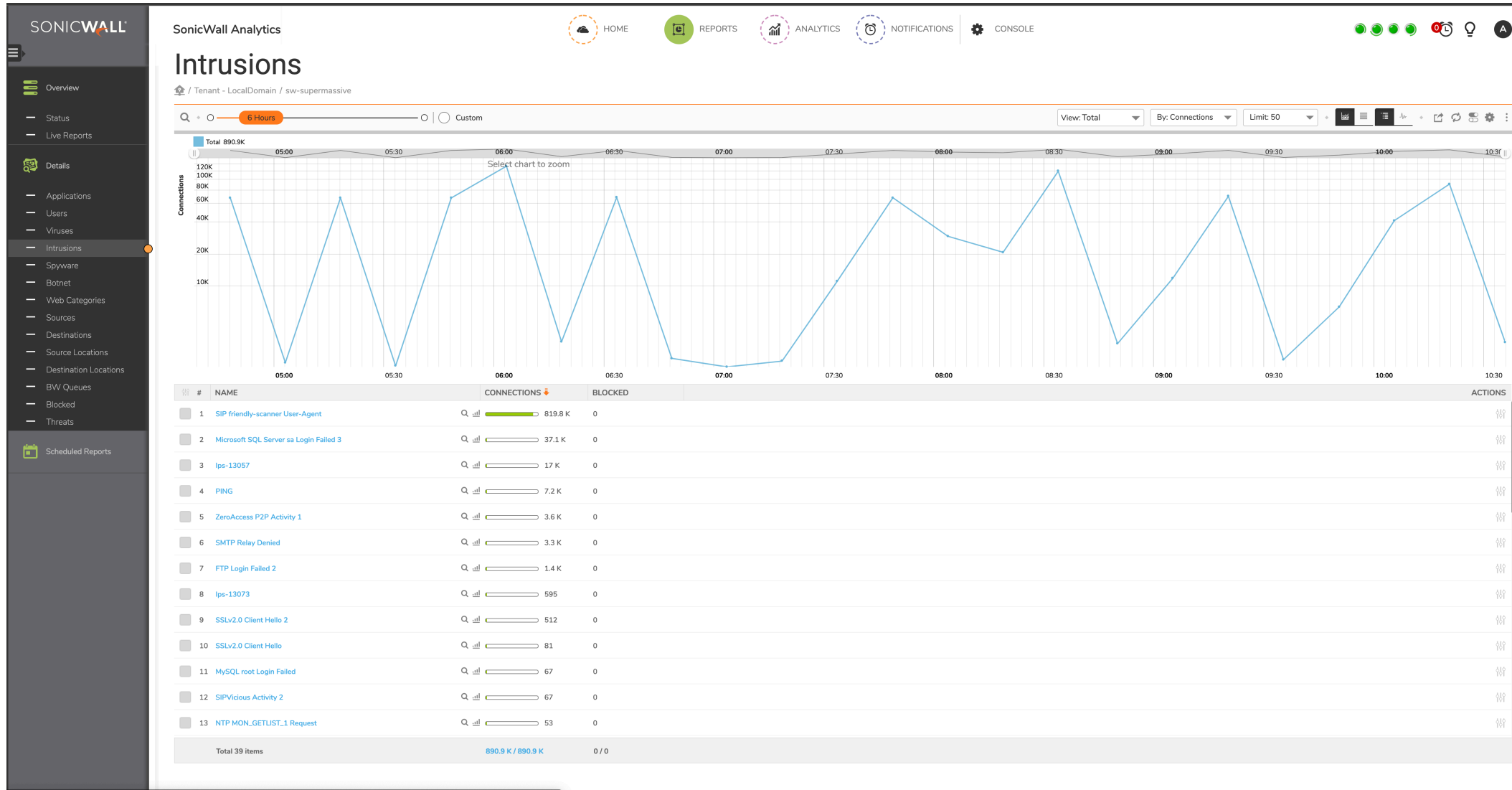
TOP APPLICATIONS BY TOTAL DATA TRANSFERRED

	APPLICATIONS NAME	TOTAL DATA TRANSFERRED	PERCENTAGE
<input type="checkbox"/>	General HTTPS	992.9 GB	54.45%
<input type="checkbox"/>	General HTTP	308.9 GB	16.94%
<input type="checkbox"/>	General LDAP	274.1 GB	15.03%
<input type="checkbox"/>	General UDP	168.3 GB	9.23%
<input type="checkbox"/>	General TCP	25.9 GB	1.42%
<input type="checkbox"/>	Service IKE (Tr...	17.2 GB	<1%
<input type="checkbox"/>	Service Edonk...	12.2 GB	<1%
<input type="checkbox"/>	General SSH	8.3 GB	<1%
<input type="checkbox"/>	Service RPC S...	8.2 GB	<1%
<input type="checkbox"/>	General DNS	7.4 GB	<1%

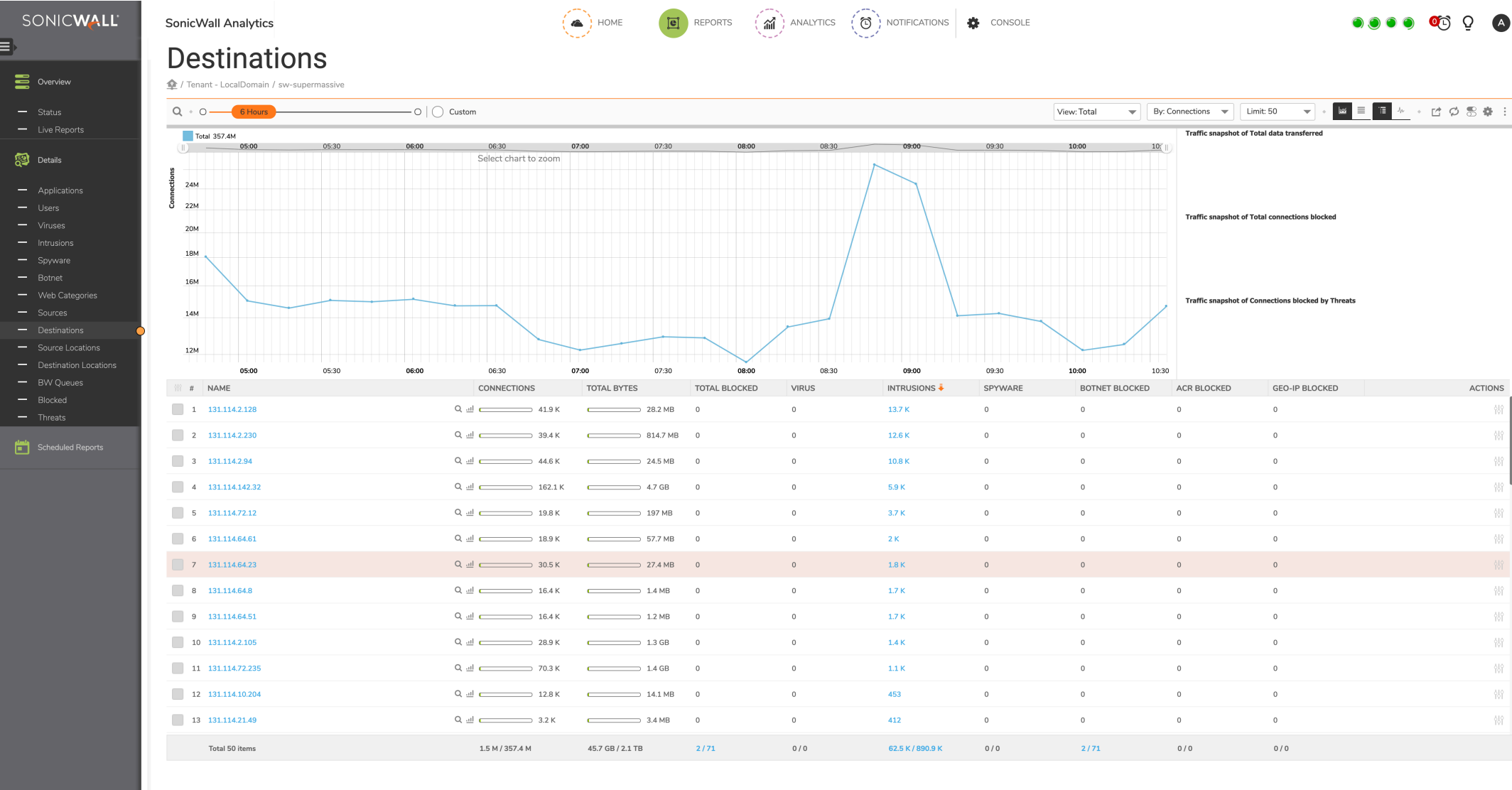
details...



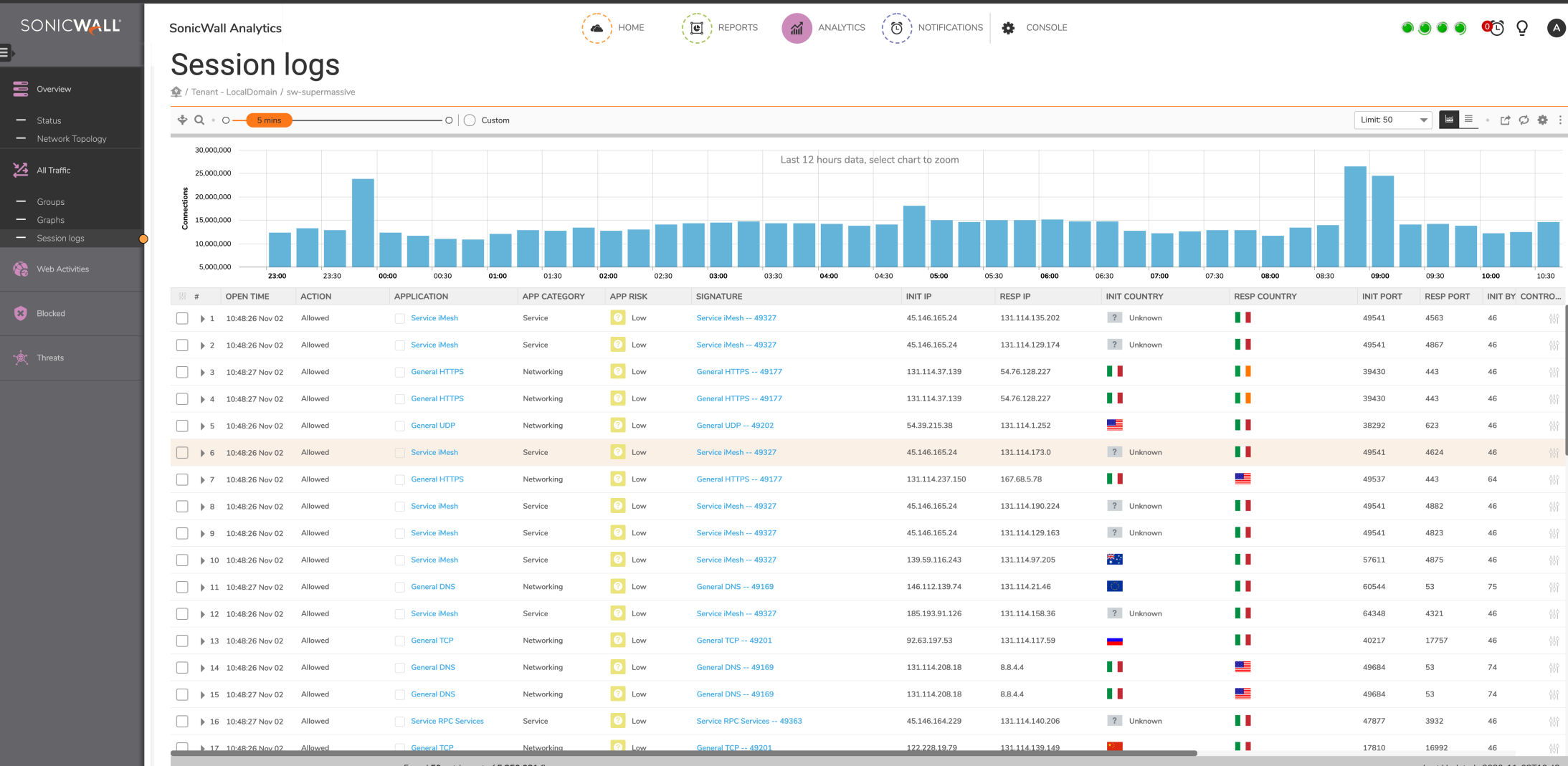
Analizing threats..Detect and non prevent..



Analizing Destination flows



Active Session Trend



Protocol Analitics

SONICWALL

Overview

Status

Network Topology

All Traffic

Groups

Graphs

Session logs

Web Activities

Blocked

Threats

SonicWall Analytics

Tenant - LocalDomain / sw-supermassive

Groups

Applications

Web Activities

Users

Sources

Destinations

Threats

Devices

BWM

Blocked

5 mins

Custom

Group by - Applications

#	APPLICATIONS	SESSIONS	TOTAL PACKETS	TOTAL BYTES	THREATS	ACTIONS
1	General HTTPS	78.3 K	7.4 M	6.6 GB	1	
2	General UDP	56.9 K	6.1 M	2.4 GB	9	
3	General TCP	201.5 K	2.1 M	1.6 GB	0	
4	General HTTP	13.1 K	709.4 K	685 MB	57	
5	General LDAP	386	119.6 K	171 MB	0	
6	General SMTP	1.7 K	97.6 K	87.6 MB	31	
7	General SSH	15.8 K	188.6 K	70.8 MB	0	
8	General DNS	74.1 K	127.4 K	21.2 MB	0	
9	Service IMAP4	438	26.8 K	17.4 MB	0	
10	Service iMesh	127.6 K	140.8 K	17.2 MB	0	
11	General SNMP	3.8 K	9.9 K	4.4 MB	0	
12	Service RPC Services	50.5 K	57.6 K	4 MB	0	
13	Service RPC Services (IANA)	64.9 K	71.9 K	3.4 MB	0	
14	General SIP control	1.2 K	4.1 K	2.7 MB	0	
15	Service Echo	10.6 K	18.8 K	1.3 MB	0	
16	Service SMB	12.8 K	16 K	877.6 KB	0	
17	General Telnet	17.1 K	18.5 K	872.1 KB	0	
18	Service NTP	5 K	5.8 K	636.4 KB	0	
19	Service Tivo TCP Data	11 K	11.6 K	545.8 KB	0	
20	Service MS SQL	10.1 K	10.7 K	512.7 KB	0	
Total 105 Items		766.3 K	17.2 M	11.7 GB	150	

22% flows scanned, Grouped 105 entries out of 1.000.004 / 4.500.028 flows

STOP

Last Updated : 2020-11-02T10:58