

STONESOFT

Network Security

Usable Security at Stonesoft

Tero Jantunen
April 26th 2011



Agenda

- Stonesoft in brief
- Usability development at Stonesoft
- Design examples
- Demo

STONESOFT

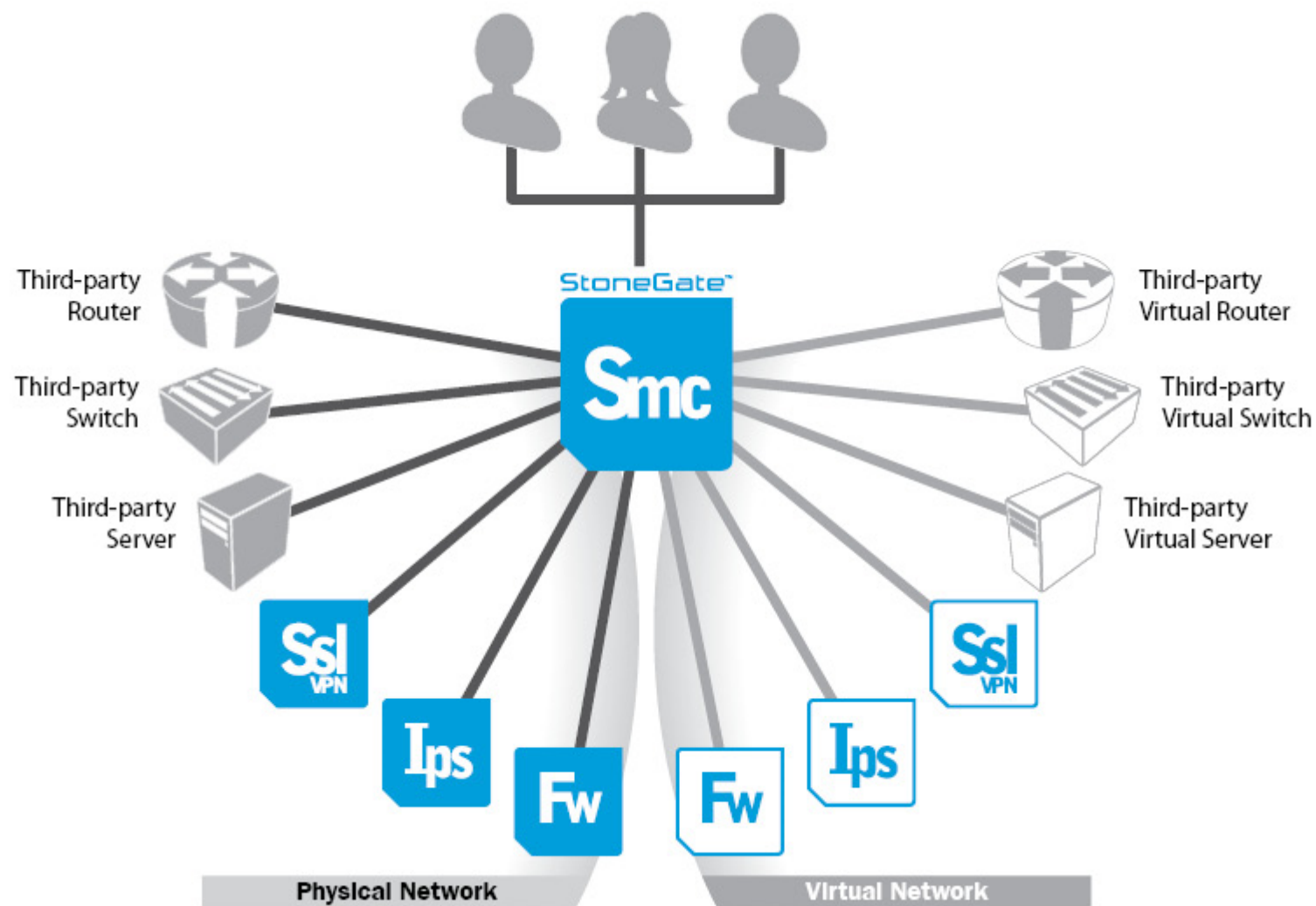
... in brief

Who are we, and what
do we produce?

Stonesoft

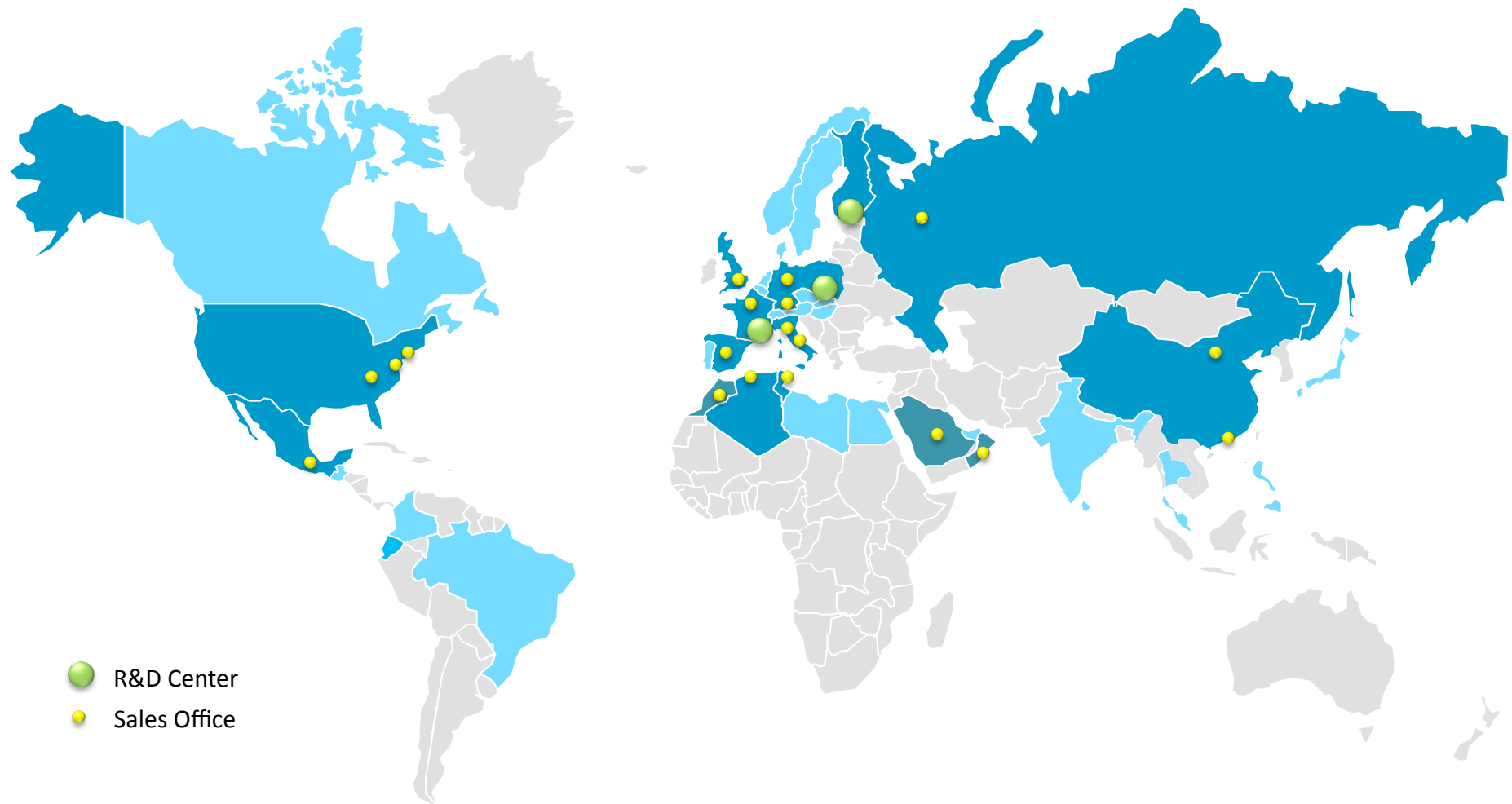
- Network Security Company
- Founded in 1990
- Number of employees: 201
- Products
 - StoneGate Firewall/VPN
 - StoGate IPS
 - StoneGate SSL VPN
 - StonGate Management Center





STONESOFT
Network Security

Geographical Coverage



Who are our customers?

- Managed Security Service Providers (MSSP)
- Large enterprises operating in geographically distributed environments
- Organizations that have high security needs

Customers we serve

Financial



Government



Technology



Legal

ARNOLD & PORTER LLP



Communications/ Utilities



Manufacturing/ Logistics



Services/Healthcare

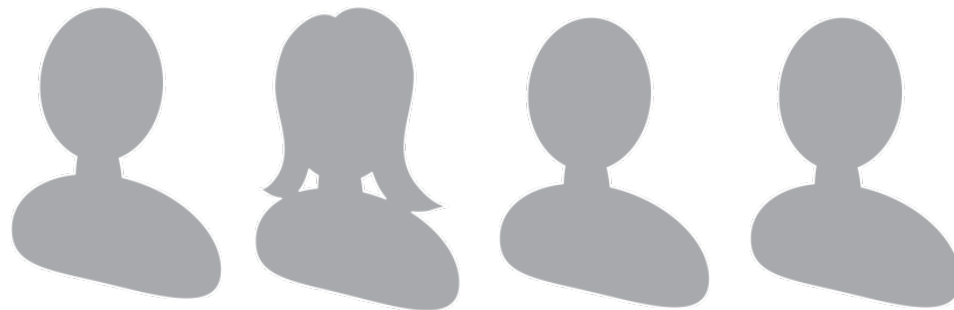


Education



Who are our end-users?

- Technical administrators that have strong knowledge of IP networks and security
 - StoneGate end users are really busy people and there are not that many end users in the first place (compared to consumer products)



Usability Development at Stonesoft

How is usability taken into account in
daily product development?

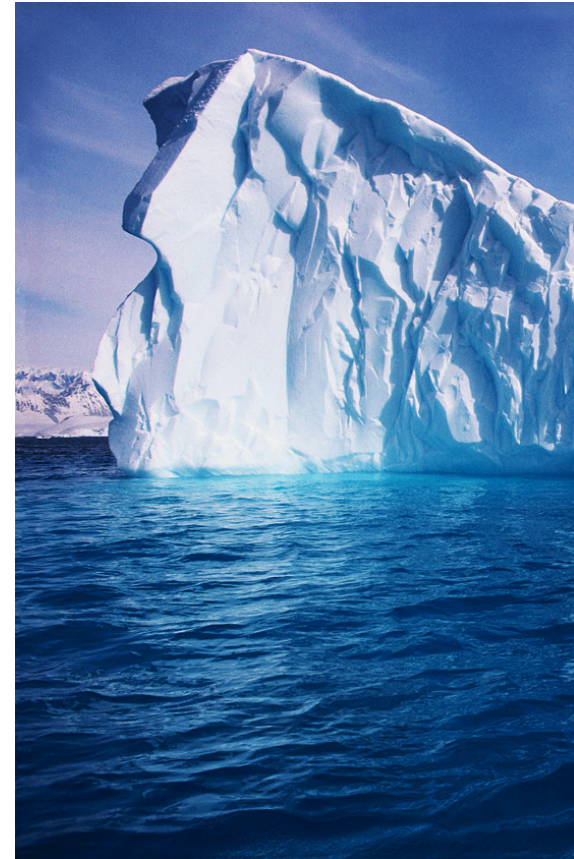
Motivation

- The user experience of StoneGate Management Center is very often the key differentiator that makes the customer to select Stonesoft as security vendor!



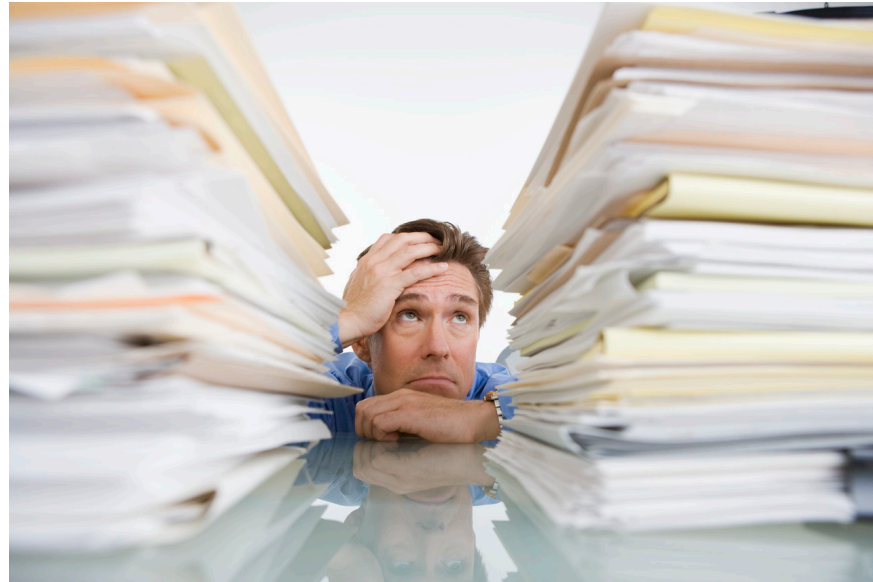
Minimize TCO

- With StoneGate Management Center the customer can manage more devices with less people in a centralized way
⇒ Lower Total Cost of Ownership



What do the customers appreciate?

- Remove routine work and automate tasks as much as possible
- Provide smooth workflows especially for the most common tasks



Interesting reading...



- Protecting the Enterprise: A Security Solution Is Only Effective If It Can Be Managed

(Gartner Research Paper written by Bob Walder ID Number: G00210354)

User-Centered Design Methods

- Interviews
- Observations
- Usability test tasks
- Questionnaires
- Heuristic evaluation



Typical customer feedback meeting is a combination of interview and observation

Design principles

1. Visibility of system status
2. Match between system and the real world
3. User control and freedom
4. Consistency and standards
5. Error prevention
6. Recognition rather than recall
7. Flexibility and efficiency of use
8. Aesthetic and minimalist design
9. Help users recognize, diagnose, and recover from errors
10. Help and documentation

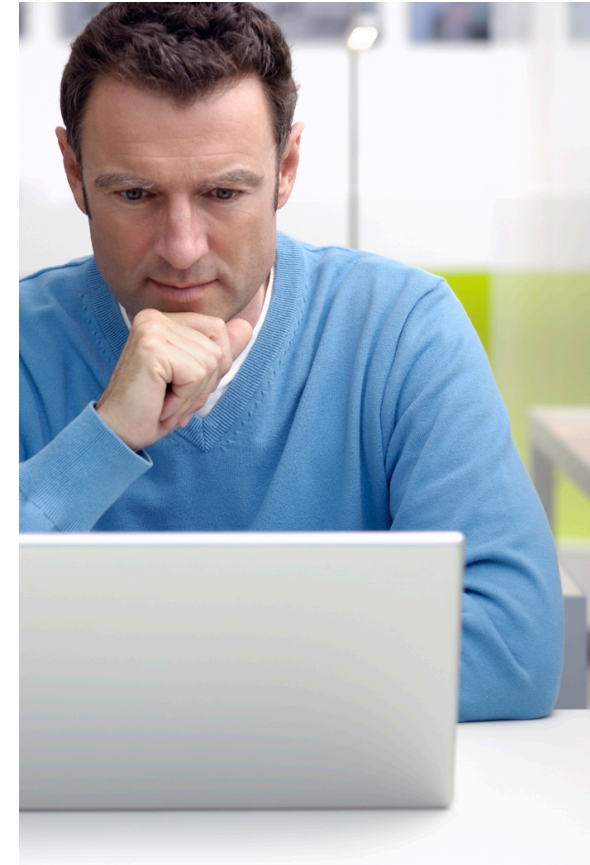


Jacob Nielsen

http://www.useit.com/papers/heuristic/heuristic_list.html

User-driven mindset

- Stonesoft R&D attends regularly to customer feedback meetings
 - E.g. Customer Technology Advisory Board
 - GUI developers also conduct usability tests
- ⇒ Each GUI developer should be aware of end users' needs and the context of use



Framework & consistency

- Try to avoid pixel-tuning as far as possible
- With a decent GUI framework you can decrease the coding effort and keep the GUI consistent
 - Increase the abstraction layer → just select which widget, sub-routine or dialog type to use
- GUI framework makes it possible to deploy big changes throughout the GUI quickly

Biggest challenges (1/5)

- Intuitivity
 - Since the StoneGate Management Center is very versatile and flexible product, it is a big challenge to make it easy to use for novice users
 - At the same time we should make sure that experienced users do not get disturbed
 - We have also noticed that the end users don't actively try to find new shortcuts and features. They use the product like they have always used.

Biggest challenges (2/5)

- Continuous development
 - We are developing a product that has existed already 10 years
 - We must keep all the existing features up and working all the time (also with old engine versions)
 - Migrations are sometimes quite tricky...

Biggest challenges (3/5)

- How to emphasize the most important pieces of data (especially in statistics)
 - The data amount can be huge
 - We should find a way to emphasize the relevant information to help administrators in decision-making or troubleshooting tasks

Biggest challenges (4/5)

- How to help administrators to keep the security policies and other parts of the management system understandable
 - Multiple administrators make modifications simultaneously
 - Some administrators may have left the company already
 - Making mistakes may stop the traffic for business critical systems

Biggest challenges (5/5)

- How to keep the GUI responsive
 - This is something that is taken for granted by the end-users
 - Not an easy task when managing massive amount of configuration, log and run-time data in high latency environments
 - Keeping the GUI responsive often means that information needs to be cached in the client side extensively

Design examples

How is usability present in
Stonesoft's products

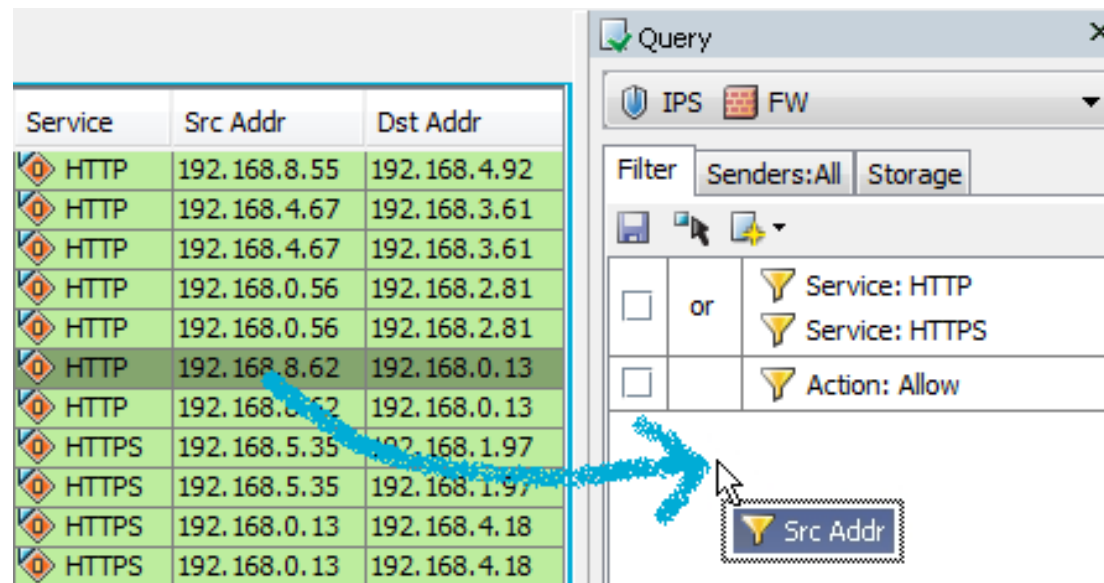
Type-Ahead Search

- Quickly find the correct elements in all contexts

14.13	All Helsinki Networks	All Helsinki Networks	ANY	Allow
14.14	Product Management	ANY	YouTube	Allow
14.15	Management	www.facebook.com	ANY	Allow
14.16	Administrators	Marketing Sales	http	Allow
14.17	Helsinki Internal Network	smcdemo.stonesoft.com	HTTP HTTP HTTP (with URL Logging) HTTP proxy HTTPS HTTPS (with decryption) Squid HTTP proxy 7 rows	Allow
14.18	ANY	Helsinki Mail Server 1 Helsinki Mail Server 2		Allow
14.19	Internal	All Internal Networks		Deep Inspection: on Anti-Spam: on Apply VPN: Corporate VPN
14.20	External	www.stonesoft.com		Allow
14.21	Product Management RAD Support	bugs.stonesoft.com		Allow

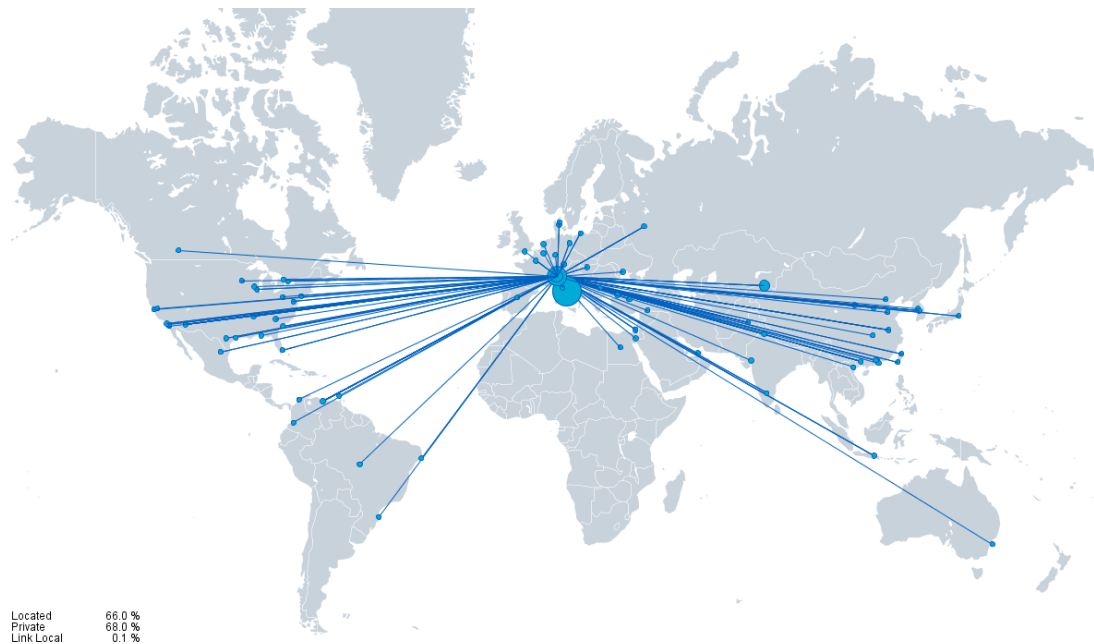
Drag & Drop Filtering

- You can troubleshoot the logs efficiently in drag & drop style



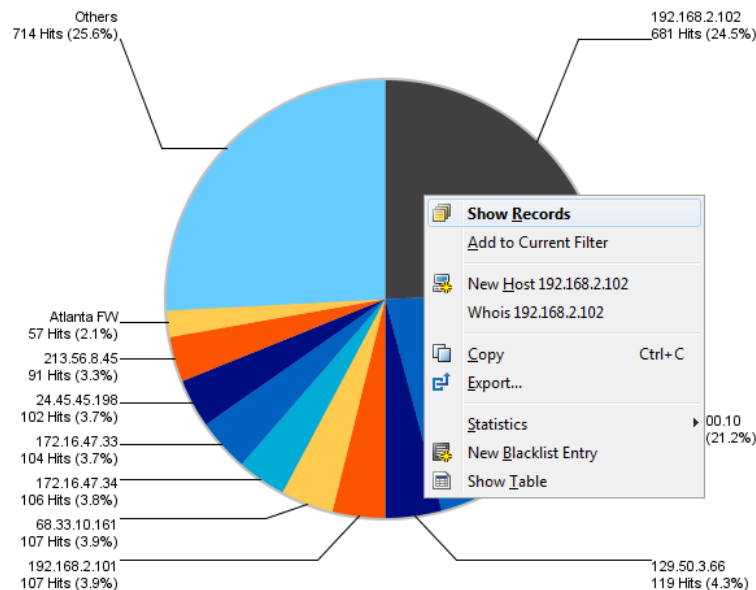
Log Visualizations

- Visualize the logs to help administrators with anomaly detection and troubleshooting tasks



Drill-In Actions

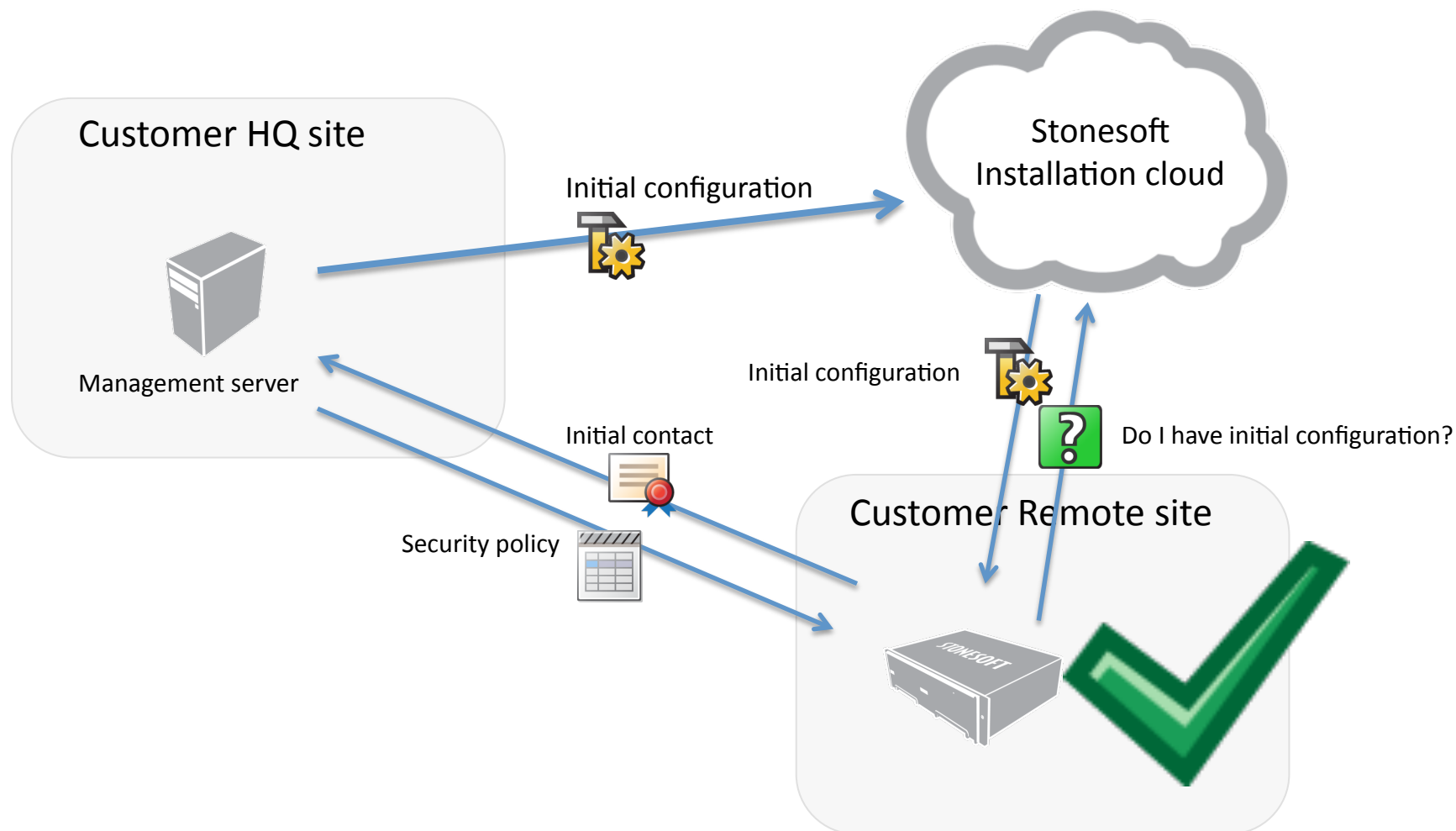
- Move efficiently between status monitoring, policies, logs, statistics and reports!



The screenshot shows the StoneSoft Network Security interface. On the left, a list of events is displayed with columns for event type, status, and IP address. A context menu is open over the 'HTTP_Request-GET' event, showing options like 'Details', 'Copy', 'View Rule', 'Create Rule', 'New Host', 'Whois', 'Print...', 'Export', 'Filter Connections', 'Search Related Events', 'New Blacklist Entry', 'Add Filter: Sender', and 'New Filter: Sender'. On the right, a table shows the details of the selected event, including the action taken (e.g., 'Permit', 'Allow', 'Discard') and the source IP address.

Event Type	Status	IP Address
HTTP_Request-GET	Permit	192.168.2.102
	Allow	192.168.2.102
	Permit	100:2::102
	Allow	10.100.100.10
	Permit	192.168.2.102
	Permit	100:2::102
	Allow	10.100.100.10
	Permit	192.168.2.102
	Discard	172.31.12.21
	Permit	100:2::102
	Permit	192.168.2.102
	Discard	172.31.13.22
	Permit	100:2::102
	Discard	172.31.11.21
	Discard	172.16.47.33
	Discard	24.45.45.198
Connection_Allowed	Allow	10.100.100.10

Plug and Play Installation



Ergonomic Authentication

- Security is never compromised
- Still solutions can be usable!



Demo time!

StoneGate Management Center

