|  |  |
| --- | --- |
|  | **Protocollo n° P-20191121 del 11/2019** |
|  | Progetto Messa in sicurezza Castellina – Step di Lavoro |
|  |  |
| 20/11/2019 | Attivazione infrastruttura di networking, security e visibilità applicativa per la nuova Materasseria ed area pulito presso l’HQ di Castellina di Soragna (PR) |
|  | **Autori:** Davide Del Bue  **Cliente:** Servizi Italia SPA  **Versione:** 1.0  **LOB:** Networking  **Revisioni:**   |  |  |  |  | | --- | --- | --- | --- | | # | Data | Modifiche |  | | 1.0 | 20/11/2019 | Prima versione | Davide Del Bue | | 1.1 | 21/11/2019 | Revisione | Davide Del Bue, Daniele Velardi, Jiaqi Sun | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |

## Step di progetto

### COMPLETATO - Sostituzione AS-IS del Cisco ASA con FGT300E;

### COMPLETATO - Upgrade banda WAN accesso internet locale a Castellina;

### Aggiunta nuove VLAN/subnet IP con relativa propagazione nella nuvola TIM

Le nuove vlan create sono le seguenti:

* Jensen tag 200
* Jensen Wan tag 201
* Christeyns tag 202
* Christeyns Wan tag 203
* AB tag 204
* AB Wan tag 205

I nuovi layer 3 creati sono:

* Jensen Wan 10.255.0.1 255.255.255.248
* Christeyns Wan 10.255.0.9 255.255.255.248
* AB Wan 10.255.0.17 255.255.255.248

### Attività da completare:

|  |  |  |  |
| --- | --- | --- | --- |
| 3.1 | Portare le nuove VLAN agli ESX | Mead | 0,5gg |
| 3.2 | Annunciare le nuove subnet | Telecom |  |
| 3.2 | Verificare gli instradamenti sugli apparati in carico Mead di Cesano | Mead | 0,5gg |

### Allargare subnet IP stabilimento da 192.168.100.0/24 a 192.168.100.0/23

### Attività da completare:

|  |  |  |  |
| --- | --- | --- | --- |
| 4.1 | Modificare subnet mask sul FGT300E di Castellina | Mead | <0,5 gg |
| 4.2 | Modificare DHCP per la rete in oggetto | IWS |  |
| 4.3 | Modificare subnet mask device con IP statico | IWS/SI/ Fornitori in base a chi gestisce il device stesso |  |
| 4.4 | Modificare annuncio verso MPLS | Telecom |  |
| 4.5 | Verificare gli instradamenti sugli apparati in carico Mead di Cesano | Mead | 0,5gg |

### COMPLETATO - Migrazione tutte le subnet/default gateway esistenti da switch/router TIM su FGT300E; cambio indirizzo IP router TIM;

### Sostituzione switch armadio C logistica; attivazione link fibra ottica fra armadio rack C logistica ed armadio H centrale termica

### Attività da completare:

|  |  |  |  |
| --- | --- | --- | --- |
| 6.1 | Verifica presenza e test link fibra disponibile tra armadio C e H | Mead | 0,5gg |
| 6.2 | Preparazione Switch, configurazione RSTP per integrarsi con gli attuali HPE | Mead | 1gg |
| 6.3 | Messa in produzione sostituendo gli switch dell’armadio C logistica | Mead | 0,5gg  Note: con 1 ora di disservizio da prevedere su tutti i device collegati a questi switch |

### Attivazione rilancio passivo per chiudere anello fra materasseria e CED: usare patch cord fibra ottica per chiudere link nell’armadio H della centrale termica; fisicamente il percorso sarà rack I – rack H – rack A;

### Premessa:

Effettuare la chiusura dell’anello sugli attuali switch prevede delle attività di configurazione RSTP, terminando la sostituzione degli switch HPE nello stabilimento con Extreme servirà configurare un nuovo protocollo, ovvero EAPS, è quindi un’opzione.

### Prerequisiti (Pre nr.7) per portare a termine l’attività:

Deve essere presente, integro ed individuabile un percorso in fibra fra materasseria e CED

### Attività da completare:

|  |  |  |  |
| --- | --- | --- | --- |
| 7.1 | Sopralluogo e test rilancio Fibra | Mead | 0,5gg |
| 7.2 | Configurazione RSTP per chiudere l’anello | Mead | 1 gg |

### COMPLETATO - Installazione nuovi macchinari JENSEN JenRail , a carico di Servizi Italia

### Attivare connettività WAN di TIM per navigazione internet locale (cambiare anche scope DHCP per non rilasciare riferimenti al file WPAD del web proxy di Cesano);

Allo stato attuale tutto è pronto per poter navigare direttamente, è però necessario che IWS smetta di rilasciare i riferimenti al file WPAD del web proxy di Cesano.

### Premessa:

Al momento la rete 192.168.160.0/23 è tutta abilitata ad accedere ad internet tramite policy, su tutti i protocolli con controlli web-filtering base, AV, IPS.

Nella rete server 192.168.36.0/24 solo i server che già in precedenza potevano accedere a Internet senza Proxy lo sono.

Nella rete di stabilimento 192.168.100.0/23 al momento nessun IP è stato abilitato a navigare direttamente.

Per identificare gli utenti che navigano attraverso il firewall è necessario installare la componente FSSO.

### Prerequisiti (Pre nr.9) :

Deve essere presa una decisione da parte di SI su chi e come deve navigare direttamente senza proxy.

Nel caso di integrazione FSSO devono essere forniti 2 server windows su cui installare il componente, predisposto un utente con diritti di admin su questi server e facente parte del gruppo di AD event log reader.

Deve essere abilitata su Active Directory l’auditing sugli eventi di logon (ID **4768,** **4769)**

### Attività da completare:

|  |  |  |  |
| --- | --- | --- | --- |
| 5.1 | Decidere quali reti dovranno navigare senza proxy | Servizi Italia |  |
| 5.2 | Decidere con quali policy di navigazione potranno farlo | Servizi Italia |  |
| 5.3 | Configurazione policy condivise | Mead | 0.5 – 3 G in base alle decisioni, 3 Giorni se si sceglie di attivare FSSO e diversificare numerosi gruppi di navigazione |
| 5.4 | Rimuovere dal DHCP il settaggio Proxy | IWS |  |
| 5.5 | Supporto Mead in caso di problematiche quando viene rimosso il proxy | Mead | 0,5gg |

### Segmentazione Rete Fornitore Jensen.

Al momento Mead ha segmentato la rete Jensen, la quale è confinata nella VLAN Jensen con tag 200, la Vlan 200 non è più sovrapposta alla VLAN di stabilimento (tag 1)

Il router Jenassist è stato portato in sala CED e termina la rete di Jensen 172.16.0.0/16, questi come da schema di collegamento Jensen comunica con il Fortigate 300 sulla rete Jensen WAN 10.255.0.0/29.

La segmentazione non è al momento completa perché esiste un apparato, chiamato server Jensen, che ha due schede di rete, una sulla rete Jensen 172.16.0.0/16 e uno sulla rete server di Castellina 192.168.36.0/24.

Tramite questo IP questo Server Jensen comunica con il server Sfera anch’esso avente IP sulla 192.168.36.0/24.

Per completare la segmentazione è necessario che la comunicazione tra questi server transiti da Jenassist e Fortigate sulla rete di comunicazione dedicata 10.255.0.0/29.

### Prerequisiti (Pre10) per portare a termine l’attività:

|  |  |  |
| --- | --- | --- |
| Pre10.1 | rimuove IP seconda scheda di rete su server Jensen | Jensen |
| Pre10.2 | configura NAT dell’IP del server Jensen sul Jenassist, utilizzando l’IP della rete di routing 10.255.0.2 | Jensen |
| Pre10.3 | configura rotta su Jenassist per cercare la rete 192.168.36.0/24 su FGT 10.255.0.1 | Jensen |
| Pre10.4 | configura regole firewall sul Jenassist per permettere comunicazione tra server Sfera e server Jensen | Jensen |
| Pre10.5 | riconfigurazione dei puntamenti su server Sfera verso IP reale server Jensen | Servizi Italia |

### Attività da completare (PIANO A CONSIGLIATO):

|  |  |  |  |
| --- | --- | --- | --- |
| 10.1 | Definire checklist test di funzionamento | Servizi Italia |  |
| 10.2 | Rimuovere IP seconda scheda di rete su server Jensen | Jensen |  |
| 10.3 | Configurare NAT dell’IP del server Jensen sul Jenbassist, utilizzando l’IP della rete di routing 10.255.0.2 | Jensen |  |
| 10.4 | Configurazione rotta su Jenassist per cercare la rete 192.168.36.0/24 su FGT 10.255.0.1 | Jensen |  |
| 10.5 | Configurazione regole firewall sul Jenassist per permettere comunicazione tra server Sfera e server Jensen | Jensen |  |
| 10.6 | Configurazione regole su Fortigate permettere comunicazione tra server Sfera e server Jensen | Mead | <0,5gg |
| 10.7 | Riconfigurazioni puntamenti su server Sfera verso IP reale server Jensen | Servizi Italia |  |
| 10.8 | Test di Funzionamento | Servizi Italia |  |

### PIANO B) Workaround se Jensen non riesce a evadere I requisiti del punto 10

Per ottenere comunque segmentazione senza le configurazioni necessarie sul Jenassist è possibile definire sul Fortigate una nuova rete Jensen DMZ, 10.255.36.0/24.

Collegare il server Jensen su questa rete al posto della rete server, lasciando una scheda di rete sulla rete Jensen 172.16.0.0/16.

In questo modo la comunicazione tra la rete server di Castellina e il server Jensen verrà comunque segmentata e regolata dal firewall.

### Attività da completare (PIANO B):

|  |  |  |  |
| --- | --- | --- | --- |
| 10.1b | Creare DMZ Jensen e configurare regole necessarie, portare la vlan fisicamente al server Jensen | Mead | 0,5gg |
| 10.2b | Configurare la scheda di rete del server Jensen con IP 10.255.36.100 | Jensen |  |
| 10.3b | Far puntare il server Sfera al nuovo IP | Servizi Italia |  |

### COMPLETATO? - Segmentazione Rete Fornitore Christeyns

Mead ha segmentato la rete del Fornitore Christeyn e veicolato l’accesso a Internet di questo tramite la Vlan **Christeyns Wan** 10.255.0.9 255.255.255.248.

È stato verificato l’accesso per l’assistenza, rimane da verificare se deve comunicare con delle reti di Castelline

### Attività da completare:

|  |  |  |  |
| --- | --- | --- | --- |
| 11.1 | Verificare se sono richieste regole per interazione con le reti di Castelline | Servizi Italia |  |
| 11.2 | Configurare eventuali policy per accesso | Mead | 0,5 - 4 H in base alle richieste |

### COMPLETATO? - Segmentazione Rete Fornitore AB

Mead portato la vlan AB WAN fino allo switch indicato da Lucchelli, ci serve un feedback per sapere se è stato collegato il device di AB al questa vlan dedicata

### Attività da completare:

|  |  |  |  |
| --- | --- | --- | --- |
| 12.1 | Contattare Lucchelli su stato dell’attività, configurare porta in access per la vlan su switch dedicato, configurare regole su | Mead | 0,5 - 4 H in base alle richieste |

### 13.Dismettere connettività dedicata ENERGYTEAM (In carico a SI)

### 14.Dismettere connettività dedicata AB (In carico a SI)

### 15.Ordine ultimi switch 2020(in carico a SI)

### 16.Sostituzione switch in produzione

L’elenco delle attività è variabile in base all’effettivo ordine che deve ancora arrivare.

Considerando circa 1 giornata per rack, oltre alla preconfigurazione dei device e l’attivazione dell’anello EAPS si prevedono circa 10 giornate.

### Attività da completare:

|  |  |  |  |
| --- | --- | --- | --- |
| 16.1 | Sostituire tutti gli switch della produzione | Mead | 9gg |
| 16.2 | Progettazione, creazione e test anello EAPS | Mead | 1gg |

### 17.Documentazione AS-BUILT

### Attività da completare:

|  |  |  |  |
| --- | --- | --- | --- |
| 17.1 | Creare schemi di rete, documentazione sul funzionamento dei vari fornitori (Jensen Chrysteyns, AB) | Mead | 2gg |